

In The Claims:

Please cancel without prejudice claim 16.

Please amend the remaining claims as follows:

- 1 1. (currently amended) A disk drive comprising:
 - 2 (a) a disk for storing data, the disk comprising a public area for storing plaintext data and
 - 3 a pristine area for storing encrypted data;
 - 4 (b) a head for reading the encrypted data from the pristine area of the disk;
 - 5 ~~(d)~~(c) a control system for interfacing with a host computer to controlling access to
 - 6 the facilitate read and write commands to write data to and read data from the pristine
 - 7 area of the disk, the control system comprising:
 - 8 authentication circuitry for authenticating a request received from an external
 - 9 entity the host computer to access the pristine area of the disk and for enabling
 - 10 the control system if the request is authenticated;
 - 11 (e) a secret drive key; and
 - 12 (f) decryption circuitry, responsive to the secret drive key, for decrypting the
 - 13 encrypted data stored in the pristine area of the disk to generate decrypted
 - 14 data.
- 1 2. (original) The disk drive of claim 1, wherein the encrypted data comprises encrypted
- 2 authentication data.
- 1 3. (original) The disk drive of claim 2, wherein the authentication circuitry is responsive to
- 2 the decrypted data.
- 1 4. (original) The disk drive of claim 2, wherein the encrypted authentication data comprises
- 2 encrypted user authentication data.

- 1 5. (original) The disk drive of claim 2, wherein the encrypted authentication data comprises
2 encrypted device authentication data for authenticating a device, the device comprising a
3 unique device ID configured during manufacture of the device.
- 1 6. (original) The disk drive of claim 2, wherein the encrypted authentication data comprises
2 encrypted information for implementing a challenge and response verification sequence.
- 1 7. (original) The disk drive of claim 2, wherein the encrypted authentication data comprises
2 encrypted message authentication data.
- 1 8. (original) The disk drive of claim 7, wherein the encrypted authentication data comprises
2 encrypted key data for generating a message authentication code.
- 1 9. (original) The disk drive of claim 1, wherein the encrypted data comprises encrypted key
2 data for decrypting an encrypted message.
- 1 10. (original) The disk drive of claim 1, wherein the encrypted data comprises encrypted
2 message data.
- 1 11. (original) The disk drive of claim 1, wherein the disk drive further comprises encryption
2 circuitry for encrypting plaintext data into the encrypted data stored in the pristine area.
- 1 12. (original) The disk drive of claim 1, wherein:
2 (a) the disk further comprises embedded servo sectors comprising servo bursts;
3 (b) the control system comprises a servo control system responsive to the embedded
4 servo sectors; and
5 (c) the authentication circuitry enables the servo control system.

1 13. (original) The disk drive of claim 12, wherein:

2 (a) the servo bursts are written to the disk in encrypted form; and

3 (b) the authentication circuitry enables the servo control system to decrypt the servo
4 bursts.

1 14. (original) The disk drive of claim 13, wherein:

2 (a) the servo bursts are written to the disk with additive noise generated from a pseudo
3 random sequence;

4 (b) the pseudo random sequence is generated from a polynomial;

5 (c) the servo control system uses the polynomial to decrypt the servo bursts; and

6 (d) the authentication circuitry provides the polynomial to the servo control system.

1 15. (canceled)

1 16. (canceled)

1 17. (currently amended) A method of processing a request received by a disk drive from an
2 ~~external entity~~ a host computer to access encrypted data stored in a pristine area of a disk,
3 the method comprising the steps of:

4 (a) using a control system internal to the disk drive to receive the request from the host
5 computer;

6 (a)(b) using the control system internal to the disk drive to authenticating the request to
7 access the pristine area and enabling to enable access to the pristine area if the request
8 is authenticated;

9 (b)(c) using the control system internal to the disk drive to reading read the encrypted
10 data stored in the pristine area; and

11 ~~(e)(d) using the control system internal to the disk drive to decrypting decrypt~~ the
12 encrypted data using a secret drive key within the disk drive to generate decrypted
13 data.

1 18. (original) The method as recited in claim 17, wherein the encrypted data comprises
2 encrypted authentication data.

1 19. (original) The method as recited in claim 18, wherein the step of authenticating is
2 responsive to the decrypted data.

1 20. (original) The method as recited in claim 18, wherein the encrypted authentication data
2 comprises encrypted user authentication data.

1 21. (original) The method as recited in claim 18, wherein the encrypted authentication data
2 comprises encrypted device authentication data for authenticating a device, the device
3 comprising a unique device ID configured during manufacture of the device.

1 22. (original) The method as recited in claim 18, wherein the encrypted authentication data
2 comprises encrypted information for implementing a challenge and response verification
3 sequence.

1 23. (original) The method as recited in claim 18, wherein the encrypted authentication data
2 comprises encrypted message authentication data.

1 24. (original) The method as recited in claim 23, wherein the encrypted authentication data
2 comprises encrypted key data for generating a message authentication code.

- 1 25. (original) The method as recited in claim 17, wherein the encrypted data comprises
2 encrypted key data for decrypting an encrypted message.
- 1 26. (original) The method as recited in claim 17, wherein the encrypted data comprises
2 encrypted message data.
- 1 27. (original) The method as recited in claim 17, further comprising the step of encrypting
2 plaintext data to generate the encrypted data stored in the pristine area.
- 1 28. (original) The method as recited in claim 17, wherein the disk further comprises
2 embedded servo sectors comprising servo bursts, the method further comprising the steps
3 of:
4 (a) servoing a head over the disk in response to the embedded servo sectors; and
5 (b) enabling servoing in the pristine area if the request is authenticated.
- 1 29. (previously presented) The method as recited in claim 28, wherein:
2 (a) the servo bursts are written to the disk in encrypted form; and
3 (b) the step of authenticating the request to access the pristine area comprises the step of
4 decrypting the servo bursts.
- 1 30. (previously presented) The method as recited in claim 29, wherein:
2 (a) the servo bursts are written to the disk with additive noise generated from a pseudo
3 random sequence;
4 (b) the pseudo random sequence is generated from a polynomial; and
5 (c) the step of servoing uses the polynomial to decrypt the servo bursts.

1 31. (currently amended) A method of processing a request received by a disk drive from an
2 ~~external entity~~ a host computer to access data stored on a disk, the disk comprising a
3 public area for storing plaintext data and a pristine area for storing encrypted data, the
4 method comprising the steps of:
5 (a) using a control system internal to the disk drive to receive the request from the host
6 computer;
7 (a)(b) using the control system internal to the disk drive to ~~decrypting~~ decrypt the
8 encrypted data stored in the pristine area of the disk using a secret drive key within
9 the disk drive to generate decrypted data; and
10 (b)(c) using the control system internal to the disk drive to ~~using~~ process the decrypted
11 data to authenticate the request received from the ~~external entity~~ host computer before
12 allowing access to the disk.

Please add the following new claim:

1 32. (new) A disk drive comprising a disk for storing data, and a head for reading data from
2 the disk, the improvement comprising:
3 a control system for interfacing with a host computer to facilitate read and write
4 commands to write data to and read data from the disk, the control system
5 comprising:
6 authentication circuitry for authenticating a request received from the host computer
7 to access the disk;
8 a secret drive key; and
9 decryption circuitry, responsive to the secret drive key, for decrypting the encrypted
10 data stored on the disk to generate decrypted data.